

NISTTech

Workflow Management Employing Role-Based Access Control

Provides access control and proper sequencing in complex networks for each activity in a workflow

Description

Role Based Access Control (RBAC) is a widely used access control model. A primary reason for this is its ease of administration as compared to other access control mechanisms. Administrators naturally think about a user's relationship to the organization in terms of the user's job responsibilities. These responsibilities constitute the user's roles within the organization. With RBAC, access is based on these roles. An administrator's organizational view is the access control mechanism.

Workflow is the partial or complete automation of a business process. Workflows consist of a set of activities carried out in a predefined order. Each activity requires privileged operations. Access to an activity is restricted to users authorized to carry out that activity. Privileged operations permitted to users can continually change during the execution of a workflow. Such requirements for administering access to activities as the workflow progresses suggest the use of RBAC as the access control mechanism based on its ease of administration. In addition, RBAC can also be used as a means of insuring that the activities which make up a workflow are carried out in the correct sequence.

NIST has developed a process, whereby a workflow management system can be created that uses an existing trusted RBAC implementation as the means to manage the execution of workflows. This process provides not only access control for each activity in a workflow, but also the proper sequencing of activities as specified in the workflow definition. As a result, this process can lower the cost of developing a workflow management system and improve the system's security by increasing the assurance that privileged operations to perform an activity within a workflow are assigned correctly.

Note: See U.S. expired parent patent # 5,414,782 under Citations below.

Applications

- **Network security and administration**
Controls access to computer networks

Advantages

- **Easy to use**
Easier to administrate compared to other access control mechanisms
- **Reduces confusion**

Intuitive process natural to the way that organizations typically conduct business

- **Saves money**

Administers access to privileged activities as they occur in sequence

Abstract

A workflow sequence specified by a process definition is managed by a workflow management system which enacts each segment in the order specified by that process definition. Role-based access control (RBAC) is used to define membership of individuals in groups, i.e., to assign individuals to roles, and to then activate the roles with respect to the process at appropriate points in the sequence. Any individual belonging to the active role can perform the next step in the business process. Changes in the duties and responsibilities of individuals as they change job assignments are greatly simplified, as their role memberships are simply reassigned; the workflow process is unaffected.

Inventors

- Barkley, John

Citations

1. Expired U.S. patent # 6,023,765

Related Items

- Process for the Enactment of Workflow Using Role Based Access Controls
- The Economic Impact of Role-Based Access Control
- Article: NIST Software Security Patent to Help Improve Health IT Privacy

References

- U.S. Patent # 6,088,679
- Docket: 96-052CPA

Status of Availability

This invention is available for licensing.

Last Modified: 07/25/2011